REMARKS

This amendment is offered in response to the Office Action of February 23, 2004.

A replacement for Figure 9 is enclosed in response to numbered paragraph 1 of the Office Action. It is respectfully submitted that the remaining figures are not hand-drawn and are sufficient for examination purposes.

In response to paragraphs 2 and 3 of the Office Action, the various claims have been amended to recite first and second "hashed digital strings" in place of "substantially unique and substantially undecryptable [first and second] digital strings". It is respectfully submitted that one skilled in the art of cryptography would understand what a "hashing function" is. Furthermore, see the paragraph bridging pages 16 and 17 of the present application. It is further respectfully submitted that this is not intended to change the intended scope of the claims, rather to serve as a clarification.

The dependency of Claims 16-18 has been amended to obviate the fourth, fifth and sixth numbered paragraphs of the Office Action.

The Office Action has rejected Claims 1-19 under 35 U.S.C. §103(a) as obvious over the Romney reference (U.S. Patent No. 5,872,848) in view of the Brown reference (U.S. Patent No. 6,671,805).

The Romney reference apparently uses digital signatures so that the receiving party can confirm that the received document is from the proper sender. However, the Romney reference offers little evidence for the sender in the face of the intended receiving party denying that the document was received or denying that the document was decrypted. Likewise, the Brown reference apparently uses documents stored with a database that are not fully encrypted. Further, the Brown reference at col. 2, lines 44-48 states that "While it would be possible to encrypt the

entire message, it would typically be too expensive in terms of time and computing resources. Consequently, for non-private communications, encrypting just the message digest is preferable." This reference does little to provide evidence that an encrypted document has been received and decrypted by the recipient.

This is quite different from the invention as claimed by newly amended Claim 1 wherein "said at least one third party, in response to a key request from said recipient, communicating to said recipient said first hashed digital string and a decryption key for decrypting output of said second encryption algorithm, said key request being recorded by said at least one third party as evidence of receipt of said electronic document by said recipient". Similarly, new Claim 20, which is dependent upon Claim 1 recites "The method of Claim 1 wherein said step of said at least one third party communicating said first and second encrypted portions to said recipient is performed in response to a data request from said recipient to said at least one third party, said data request being recorded by said at least one third party".

Similarly, newly amended Claim 7 recites "transmitting a key request for a decryption key for said second encryption algorithm, said key request including said message identifying number, said key request further serving as evidence of receipt of said electronic message and decryption of said first encrypted document portion". New Claim 21, which is dependent upon Claim 7, recites "The method of Claim 7 wherein said step of receiving is preceded by a step of requesting communication of said encrypted electronic message and a message identifying number in response to notification of said encrypted electronic message."

Independent Claims 10 and 15 recite a method of generating an evidentiary trail, the steps of which are clearly not disclosed in the cited prior art.

The presently claimed invention can be implemented to result in a high speed electronic secure communication system with an audit trail and evidentiary quality verifiability that was modeled on certified mail. This system establishes that the document that was sent was the one that was received, read and verified by the recipient to an independent registry and to the sender. Additionally provided, in Claim 13, is document verifiability of the plaintext version of the transmitted document through the use of message identifying numbers.

For all of the reasons above, it is respectfully submitted that all of the presently pending claims are in immediate condition for allowance. The Examiner is respectfully requested to withdraw the rejections of the claims, to allow the claims, and to pass this application to early issue.

Respectfully submitted,

Ronald E. Brown
Registration No. 32,200